UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DISTRICT

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	No. 4:16-CR-258 CEJ (NAB)
	)	
ALDEN DICKERMAN,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE AND STATEMENTS

Comes now the United States of America, by and through its attorneys, Richard G. Callahan, United States Attorney for the Eastern District of Missouri, and Colleen Lang, Assistant United States Attorney for said district, and files its Response to Defendant's Motion to Suppress Evidence and Statements.

I. INTRODUCTION

Defendant moves to suppress evidence seized from Defendant's residence by law enforcement officers. Defendant specifically claims that the items seized from the defendant's residence were seized pursuant to a state search warrant issued without probable cause. Further, the defendant argues that the evidence seized and searched by law enforcement were "fruit of the poisonous tree" resulting from an illegal search and arrest and should be excluded.

The affidavit in support of the search warrant was supported by ample probable cause and did not contain false statements. The search warrant was executed properly and the evidence was properly searched.

II. FACTUAL BACKGROUND[1]

A. Background on Freenet and Law Enforcement Investigations on Freenet

In September of 2011, Special Investigator ("S.I.") Wayne Becker of the Dent County Sheriff's Department began to collect "keys" and files of child pornography located and being shared on "Freenet." In April of 2012, Special Investigator ("S.I.") Wayne Becker of the Dent County Sheriff's Department began to review logs for requests of files containing child pornography on Freenet in order to find individuals who were looking for and sharing child pornography on Freenet. Freenet is a type of peer-to-peer network software that allows users to share files over the Internet. It uses a decentralized, distributed data store to keep and deliver information. It is free and publicly available software for publishing and communicating on the Internet. Freenet's focus is to provide a place on the Internet for free speech and anonymity. In Freenet, each file is made up of several blocks, or splits, that are stored independently of each other. To view a file, you must request all the blocks that are necessary to reconstruct it. The keys used to identify a block to retrieve are the hash values of the blocks. Users contribute to the network by giving bandwidth and a portion of their hard drive for storing files. Freenet transmits data between nodes, also known as peers. Freenet also stores data on the nodes. The process of finding a piece of data, or a place to store data, is called routing. Nodes are the computers running Freenet. A node in Freenet interacts directly with its directly connected peers. Each peer's IP address is visible to a node, but a node does not learn the IP addresses of its peers' peers. On the current version of Freenet, a node may have up to 142 peers. (See Exhibit 1, "Statistical Detection of Downloaders of Child Exploitation Materials in Freenet" for more detail

[1] The background and factual summary information provided is intended as a general guide to aid the Court. It is not intended as a comprehensive statement of the government's case.

on Freenet).

Researchers and law enforcement studied the Freenet open source code and analyzed activity on Freenet. Through their study they were able to create a statistical algorithm to determine the likelihood that a peer is the requestor of child pornography files, versus being a peer that only relayed the request. The timeline for these activities are as follows. Beginning in 2012, S.I. Becker collected keys in order to build database of files on Freenet that are associated with known or suspected child pornography images and videos. Researchers at the University of Massachusetts Amherst helped modify the Freenet program for law enforcement use. The modification logs the IP address, the content hash key values, the hops-to-live ("HTL"), types of requests, and the date/time of the requests as it passes through the node. Back in 2012 and 2013, this information was then collected by SI Becker's ICAC lab in Salem, Missouri. SI Becker analyzed that information to determine if the IP address appeared to be the likely requester of known child pornography files on Freenet.

SI Becker began investigating child pornography offenders on Freenet in 2012 and 2013. In 2014, the research staff at University of Massachusetts Amherst worked with SI Becker to develop a new method to determine if an IP address appeared to be requesting known child pornography files on Freenet.

In 2015, these researchers developed a statistical algorithm for determining whether a peer is more likely to be requesting child pornographic material on Freenet or relaying such a request. This algorithm was still being refined at the time of SI Becker's investigation into the defendant's requests for child pornography on Freenet. At the time of investigation into the defendant, SI Becker was using a method that is fundamentally similar to what the algorithm does now because both methods count requests for blocks that make up a file of known child pornography. A count of requests distinguishes the requesters from relayers.

While Freenet tries to be a harbor for anonymity, the website warns about the possibility that an IP address could be recognized. The website states, "If you are connected to a node, and can recognise the keys being requested (probably because it was posted publicly), you can show statistically that the node in question probably requested it, based on the proportion of the keys requested from that node, the locations of nearby nodes, the HTL on the requests and so on.[2]" The warning is basically what law enforcement is doing – recognizing known keys and determining whom is a requestor versus a relayer by the number of blocks being requested.

The mathematical algorithm that is currently in use for the law enforcement version of Freenet is laid out in further detail in the article, "Statistical Detection of Downloaders of Child Exploitation Materials in Freenet," and was written in July of 2016. Exhibit 1. The method the algorithm uses is very similar to the method that SI Becker used in 2015. The article sums up the algorithm as follows, "[b]riefly, the algorithm works by looking at the cumulative number of requests for blocks corresponding to a distinct file of interest made by any single node. It then calculates whether the number of requests observed is most likely what we would expect to observe if the peer were the originator of the request or just replaying request on behalf of other nodes." Ex. 1, page 4, section 4.

[2] Warning from the Freenet Project webpage (https://wiki.freenetproject.org/FAQ).

B. Instant Offense

While investigating Freenet requests on April 2, 2015, S.I. Becker came across a computer with an IP address in the state of Missouri that requested a file of known child pornography. SI Becker documented the data related to that IP address' request for the file of child pornography on Freenet. Exhibit 2, SI Becker's Excel Spreadsheet. S.I. Becker collected the file and IP address information and sent it to Det. Michael Slaughter of the St. Louis County Police Department who sent a subpoena to AT&T Internet services to determine the subscriber information for that IP address. AT&T responded that the name and address of the subscriber was Janis Dickerman at 9524 Corregidor Drive, St. Louis, Missouri, 63134.

A computer search of the address revealed that Janis Dickerman had Ameren UE utilities in her name at that residence since 1959. A search warrant was prepared by Det. Slaughter and signed by St. Louis County Judge Borbonus on August 18, 2015. The search warrant stated "While reviewing requests received by undercover Freenet nodes, located in Missouri, SI Becker observed IP address 172.12.235.62 routing/or requesting suspected child pornography blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requestor of the file." Exhibit 3, Search Warrant Affidavit, ¶ 6. "SI Becker observed that on April 2, 2015, between 11:08 p.m. UTC and 11:10 p.m. UTC a computer running Freenet software, at IP address 172.12.235.62, requested from Freenet law enforcement nodes 69 parts, or blocks, of the following file." Ex. 3, ¶ 7. The affiant then identified that file with its' name and unique SHA1 hash value. The file was then described as a folder containing seventeen (17) images of a young prepubescent child in a lascivious display of her genitals and being anally penetrated. In paragraphs twelve (12) through twenty-two (22) of the search warrant affidavit, Freenet was described and explained at length. Ex. 3.

The search warrant was executed by St. Louis County Police on August 18, 2015, at 9524 Corregidor Drive, St. Louis, Missouri. The defendant, Alden Dickerman, was the only person home during the execution of the warrant. After being read his *Miranda* warnings, the defendant told police that he lived in the home with his mother (Janis Dickerman) and his sister. The defendant stated that he owned three computers including a laptop. He stated that he was only user of his laptop, which was password protected. Further, the defendant told Det. Slaughter that he had used Freenet software. When asked about downloading pornography from Freenet, the defendant asked for an attorney and questioning about the case ceased.

Meanwhile Det. Partney and S.I. Becker searched the home for computers and computer-related devices. They previewed the defendant's computers at the residence to see if they contained child pornography. These computers were located in the defendant's bedroom. Two of the defendant's computers did not contain child pornography. A third computer belonging to the defendant was an Asus laptop computer that was password protected. Detectives located a typed list of passwords in the defendant's bedroom and were able to use one of the passwords to access the Asus laptop. S.I. Becker determined the Asus laptop contained Freenet software and files of child pornography.

On August 21, 2015, S.I. Becker began a forensic review of the Asus laptop. S.I. Becker is a qualified forensic examiner. S.I. Becker located 597 images of child pornography and 43 videos of child pornography on the defendant's laptop computer's Hitachi hard drive. Freenet and the related Frost software were also located on the laptop. Frost is a group message board that relies on the Freenet peer-to-peer network. S.I. Becker also found that the defendant was subscribed to three boards on Frost, "pthc," "lolicam," and "hurtcore." The titles of the boards are indicative of child pornography. Many of the images and videos found on the laptop depicted prepubescent minor children, under the age of twelve, engaging in sexually explicit conduct. S.I. Becker noted that about thirty-two (32) of the images and nine (9) of the videos depicted the sex abuse of children as young as toddlers or infants. Many of the images and videos also portrayed sadistic or masochistic conduct.

On June 22, 2016, a federal grand jury indicted the defendant on one count of Possession of Child Pornography in violation of Title 18 U.S.C. Section 2252(a)(5)(B).

III. **LEGAL ANALYSIS**

A. **The Search Warrant was Issued on Probable Cause and Was Not Based Upon Misleading Statements, Conclusory Statements, or Omissions**

Defendant argues the evidence seized from the residence should be suppressed on the grounds that the search warrant lacked probable cause because it was issued as a result of false and misleading statements and omissions pertaining to Freenet. This argument is belied by the affidavit itself. The search warrant affidavit in this case provided sufficient probable cause.

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV. The issue before the court when reviewing the legal sufficiency of the basis for the issuance of a search warrant is whether the issuing judge had a substantial basis for concluding that probable cause existed. *United States v. White*, 356 F.3d 865, 869 (8th Cir. 2004); *United States v. Terry*, 305 F3d 818, 823 (8th Cir. 2002).

"[P]robable cause does not demand the certainty we associate with formal trials." *Illinois* *v. Gates*, 462 U.S. 213, 246 (1983). The determination of probable cause is made by a "totality of the circumstances" review. *Id.* at 238. In the context of a search, probable cause is defined as a "fair probability that contraband or evidence of a crime will be found in a particular place." *Id.* The reviewing magistrate is to consider the facts in a practical common sense manner. The evidence must provide the magistrate with a "substantial basis" for his findings. *Id.*,238-9.

In this case, the affidavit provided sufficient probable cause and is not based on false or misleading statements or omissions of fact. The Eighth Circuit has held that defendants must prove that false statements were made and "may not infer bad motive absent even a scintilla of material fact supporting that inference." *Morris v. Lanpher*, 563 F.3d 399, 403 (8th Cir. 2009). In our case, the defendant alleges that the affiant misrepresented the accuracy of SI Becker's findings. He provides no proof that his allegations are true, nor does the defendant claim that even if the statements were erroneous, the officer believe they were erroneous and made them anyway.

i. <u>Government's Response to Alleged Misrepresentations in the Search Warrant</u>

The defendant points to this statement in particular in the search warrant affidavit claiming it is misleading, "[t]he number and timing of the requests was significant enough to indicate that the IP address was the apparent original requestor of the file." The defendant then states, while relying on an affidavit by Steven Dougherty, that law enforcement left out that additional steps needed to be taken to determine that the pattern observed was not the result of a bad connection. Defendant goes onto say that the statement is misleading because it represented the only explanation for the number and timing of requests. That is clearly not what the statement represents. The statement from the affidavit is not misleading nor false. The full paragraph reads, "While reviewing requests received by undercover Freenet nodes, located in

Missouri, SI Becker observed IP address 172.12.235.62 routing/or requesting suspected child pornography blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requestor of the file." Ex. 3, ¶ 6. Nothing about that statement is false. The statement does not say the *only* explanation for the number and timing of these requests originating from the is IP address is that the IP address was initiating the requests for these file blocks that contained suspected child pornography. It represents that that the requests from that IP address *were significant enough* to indicate that the IP address was the *apparent* original requestor of the file of child pornography.

Further, an explanation of how files are requested on Freenet is explained in the search warrant affidavit. As is detailed in the search warrant affidavit in paragraphs sixteen (16) and twenty-one (21), Freenet "will receive requests from other computers running Freenet containing the key of a part of a file to retrieve from the node's data store, or to forward to another user that may have that part of the file." Ex. 3, ¶ 16. "The affiant knows from training and experience that streams of requests for blocks of a particular file from an IP address can be evaluated to determine if the IP address is the likely requestor of the file." Ex. 3 ¶ 21. Those statements represent that the blocks, or parts of the file, are coming from different nodes, or different computers. The blocks then stream to the requestor where when assembled together, can be viewed as a document, image or video file. The number and timing of the requests for those blocks from a particular peer, in this case the defendant, was significant enough to determine the defendant was the likely requestor of the file. While using a law enforcement version of Freenet modified by the researchers at University of Massachusetts Amherst to passively log observations, SI Becker could observe the streams of data coming from a Freenet node at the defendant's IP address. This significant data included information such as the time and frequency of requests for certain files of interest from a node. See Ex. 2. SI Becker then reviewed the significant data and calculated the percentage of even share. Ex. 2. The higher the percentage of even share and the more requests per second there are for a file of interest – the more likely the requests are coming from the requestor and not a forwarder. Ex. 1, Section 3 and Ex. 2. In this case, the law enforcement node, "LE #693," received 69 requests for a file that when complete contain 783 data blocks. Thus, 8.81% of the minimum necessary requests went through the law enforcement node on Freenet from the defendant's IP address. The defendant had an average of 56.9 peers during the period of investigation (which includes the law enforcement node). On average, each peer would expect to receive an even proportion (i.e. share) of requests. If the defendant had been a relayer rather than a requestor, the law enforcement node would have received a much smaller percentage of the requests. The process was repeated three times for three separate files on three separate days. Ex. 2. Therefore, Detective Slaughter's statement in the affidavit that "[t]he number and timing of the requests was significant enough to indicate that the IP address was the apparent original requestor of the file" is a correct and true. Based on the data streams, the defendant's IP address appeared to be the requestor of the file, not another node on Freenet. There are no misrepresentations in the search warrant affidavit.

ii. Government's Response to Alleged Omissions in the Search Warrant

Defendant also alleges there are omissions in the search warrant affidavit. Specifically, the defendant alleges that relevant discussion regarding the behavior of Freenet's routing in estimating the probability that received requests originated from the peer they were received from and a discussion about false positives that might have resulted during SI Becker's undercover operation on Freenet were omitted from the search warrant affidavit. The defendant does not show that the omitted facts were intentionally left out to make the affidavit misleading nor how by supplementing the omitted information, there cannot be a finding of probable cause.

The defendant must offer some evidence beyond mere assertions that an officer made an omission in the affidavit. *United States v. Castillo*, 287 F.3d 21, 26 (1st Cir. 2002).

Omissions are different then misrepresentations and require a different two-step test. The defense "must prove first that facts were omitted with the intent to make, or in reckless disregard of whether they make, the affidavit misleading, and, second, that the affidavit, if supplemented by the omitted information, could not support a finding of probable cause." *United States v. Allen*, 297 F.3d 790, 795 (8th Cir. 2002).

First, discussions on the probability that the received requests originated from suspect computer versus another elsewhere was not intentionally left out of the warrant to make it misleading. SI Becker kept notes on the data streams coming from defendant's IP address. Ex. 2. The law enforcement version of Freenet that SI Becker utilized collected this data. The review of the data by SI Becker leads him to be able to detect child pornography requestors on Freenet. The affiant wrote that based on the "number and timing of the requests" it was significant enough to indict that the IP address was the apparent original requestor of the child pornography file. In this case, SI Becker saw that the law enforcement node received 8.81% of the minimum number of requests for 783 data blocks had been divided up evenly between 56.9 peers. A similar statistical result was observed by SI Becker for two additional files. Ex. 2. The statistical application is that the defendant's IP address was a peer to the law enforcement node and had to be the one making the requests.

Second, the defendant alleges there is a potential for false positives that might have resulted and that should have been in the search warrant affidavit. In this case, false positives did not result. No false positive rate has been established for the exact method SI Becker was using in 2015, however, that method is similar to the one documented in Ex. 1. In July of 2016, a false positive rate was estimated by the researchers from University of Massachusetts at Amherst for the method described in Exhibit 1. In a test sampling four months of data, they observed a false positive rate of 1.35%. Plus, in this case, both Freenet and child pornography files were located on the defendant's computer during the execution of the search warrant – confirming that the search warrant was not based on a false positive result. Further, SI Becker logged the defendant's IP address requesting files containing child pornography two others times in June of 2015. Ex. 2. By running three separate tests, SI Becker reduced the probability of a false positive in his conclusion that a computer at this IP address had been the apparent originator of requests for child pornography. The defendant makes a blanket statement not supported by any facts, that "false positives are likely to occur."

The affidavit of Steve Dougherty referenced by the defendant and attached to his motion does not explain how "false positives" occurred in this case. Dougherty's affidavit states that poor or slow Internet connection might affect routing on Freenet. Dougherty goes on to state that at the end of affidavit that "whether the claim that 'the number and timing of the requests was significant enough to indicate that the IP address was the apparent original request or of the file' is based on sound reasoning and observation." SI Becker used sound reasoning and did observe the requests. Therefore, based upon the defendant's experts own statements, the analysis was performed correctly. Dougherty goes on to state that he had to read an additional paper supplied by the prosecutor to learn sufficient details. Dougherty was provided SI Becker's notes, Exhibit 2, and the article attached as Exhibit 1 to this response. Dougherty is not faulting anything in SI Becker's notes and, therefore, is basically acknowledging the additional information in the notes and from the article supports the findings.

In paragraph sixteen (16) of Dougherty's affidavit he alleges that the law enforcement node on Freenet might receive more requests because it may be more reliable than the other nodes, causing skewed results. However, if the target node is actually a forwarder node rather than the original requester, it would only receive a subset of the requests to begin with and the target's node would still have other peers to choose from, not just the law enforcement node, so the number of requests seen by the law enforcement node would still be greatly reduced if the target were actually a forwarder. On April, 2, 2015, the law enforcement nodes saw a proportionally large amount of requests for a file of child pornography, coming from the defendant's IP address, which shows that he was likely the requestor not a forwarder. Exhibit 2.

The very detailed specifics on how the modified version of Freenet for law enforcement worked in observing the defendant's traffic was not necessary for the search warrant affidavit. A search warrant affidavit does not have include every single detail of the investigation, it just must have enough to support probable cause. The affidavit "should be examined under a common sense approach and not in a hyper technical fashion." United *States vs. Solomon*, 432 F.3d 824, 826 (8th Cir.2005) quoting from *United States v.* Williams, 10 F3d 590, 593 (8th Cir.1993). The omissions, which is basically the raw data backing up SI Becker's deductions, only bolsters the probable cause when supplemented into the search warrant affidavit.

B. The Judge Authorizing the Warrant was a Neutral Party and Was Capable of Determining Probable Cause.

Warrants may only be signed by an official who is "neutral and detached" and "capable of determining whether probable cause exists for the requested arrest or search." *Shadwick v. City of Tampa*, 407 U.S. 345, 350 (1974). In *Shadwick*, the city authorized municipal clerks, who were supervised by Judges, to issue arrest warrants for ordinance violations. The Supreme Court of the United States affirmed lower court rulings the clerks were quailed to make a probable cause determination to issue the warrants. The Supreme Court in *Shadwick* stated:

> “Appellant likewise has failed to demonstrate that these clerks lack capacity to determine probable cause. The clerk's authority extends only to the issuance of arrest warrants for breach of municipal ordinances. We presume from the nature of the clerk's position that he would be able to deduce from the facts on an affidavit before him whether there was probable cause to believe a citizen guilty of impaired driving, breach of peace, drunkenness, trespass, or the multiple other common offenses covered by a municipal code. There has been no showing that this is too difficult a task for a clerk to accomplish. Our legal system has long entrusted nonlawyers *352 to evaluate more complex and significant factual data than that in the case at hand. Grand juries daily determine probable cause prior to rendering indictments, and trial juries assess whether guilt is proved beyond a reasonable doubt. The significance and responsibility of these lay judgments betray any belief that the Tampa clerks could not determine probable cause for arrest.” *Shadwick v. City of Tampa*, 407 U.S. 345, 351–52 (1972).

The material set forth in the affidavit relies upon technical computer information, but does not require that either the affiant who prepared the affidavit or the judge who reviews that affidavit have a requisite level of expertise in computer science before rendering a judgement. As the Supreme Court in *Shadwick* noted, our justice system relies on grand juries and trial juries, made up of ordinary citizens, to render judgements in complex and technical cases. If the justice system relies on ordinary citizens to make judgements in complex matters, then an experienced judge, even if lacking expertise in computer science, can also determinate whether probable cause exists in a search warrant affidavit for child pornography.

Defendant alleges that due to Judge Borbonus, “apparent lack of training in topics related to *Freenet* and complex computer networking, he was not in the position to test the factual basis of the affidavit.. .” Defendant’s Motion to Suppress, page 7. The search warrant affidavit read by Judge Borbonus describes how Freenet works in paragraphs sixteen (16) through twenty-two (22). Ex. 3. A reading of the search warrant affidavit does not necessitate a scientific background. A search warrant in a murder investigation does not require that the affiant have a background in pathology to indicate the cause of death was blunt force trauma nor does the magistrate have to have such a background to review and sign a search warrant in a murder case. Similarly, a search warrant for synthetic drugs not mean that the magistrate judge has to be an expert in organic chemistry.

Defendant goes on to allege in his motions the Judge's approval, "served as a rubber stamp for police." This a baseless and completely unfounded allegation supported by no facts. The defendant does not present any evidence showing that Judge Borbonus compromised his ethics and judicial obligation to sign a search warrant in collusion with the police and in violation of the defendant's constitutional rights. The defendant has made no attempt to show that the Judge was not a neutral, unbiased party. The defense cannot simply state that a judge is not neutral, they must point to something in the record that proves this. *United States v. Farlee*, 757 F.3d 810, 820 (8th Cir.), cert. denied, 135 S. Ct. 504, 190 L. Ed. 2d 379 (2014).

An issuing judge's "determination of probable cause should be paid great deference by reviewing courts" and should be upheld if the judge had a "substantial basis for ... conclud[ing] that a search would uncover evidence of wrongdoing." *Gates*, 462 U.S. at 236, 103 S.Ct. 2317 (alteration in original) (internal quotations omitted). There is no reason to believe that Judge Borbonus was biased or incapable of signing the search warrant.

C. The Search Warrant Did Contain Enough Facts to give the Issuing Judge a Substantial Basis for his Determination of Probable Cause.

In his third point in his motion to suppress evidence, the defendant argues that the warrant failed to provide the magistrate with a substantial basis for determining the existence of probable cause. In other words, the defendant is again arguing that there were omissions in the search warrant. Not every detail of the investigation must be in the search warrant. Det. Slaughter tells the reviewing Judge in paragraph two (2) of the search warrant affidavit that, "this affidavit is being submitted for the limited purpose of securing a search warrant, your affiant has not included each and every fact concerning this investigation." Ex. 3, ¶ 2. The search warrant in the case did provide sufficient information to form probable cause for the reviewing Judge.

> "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others. In order to ensure that such an abdication of the magistrate's duty does not occur, courts must continue to conscientiously review the sufficiency of affidavits on which warrants are issued. But when we move beyond the "bare bones" affidavits present in cases such as *Nathanson* and *Aguilar*, this area simply does not lend itself to a prescribed set of rules, like that which had developed from *Spinelli*. Instead, the flexible, common-sense standard articulated in *Jones*, *Ventresca*, and *Brinegar* better serves the purposes of the Fourth Amendment's probable cause requirement." *Gates*, 462 U.S. at 239.

The search warrant in this case contained the background and expertise of both the affiant, Det. Slaughter, and the investigator, SI Becker. It then explains in several paragraphs SI Becker's investigation into child pornography activities on Freenet. Ex 3, ¶ 4, 5. The search warrant than details the crime, specifically that on April 2, 2015, between 11:08p.m. UTC and 11:10p.m. UTC, the IP address of 172.12.235.62 requested a known file of child pornography. The affiant that lists the file name, hash value, and description of the file of child pornography that was requested. Ex. 3, ¶ 6, 7. The affiant than confirms that he also reviewed the requested file of child pornography and came the same conclusion as SI Becker, that it was in fact child pornography. The affiant then details in paragraphs nine (9) and ten (10) that AT&T Internet Services provided the subscriber's name, and address for that IP address. Affiant also states that utility company shows the subscriber living at the address since 1959. The remaining thirteen (13) paragraphs then describe how Freenet peer-to-peer networking works and how individuals who collect child pornography act. The search warrant was not based on bare conclusions. It contains details on how a crime was committed, when it was committed, where it was committed, and by a person at a certain address. The search warrant affidavit described how the IP address was the nexus that connected the contraband and the home that was searched.

The defendant again alleges in this third section of his motion that there were factual misrepresentations in the affidavit. The Government has fully explained earlier in this response how this is untrue and that the search warrant contained sufficient, correct, and reliable information. The only possible conclusory statement in the search warrant is in paragraph six (6), which states that the number and timing of the requests "were significant enough." They were significant enough to make a determination that it was the defendant's IP address and not another node on Freenet that requested the file of child pornography. That is not improperly conclusory.

The Supreme Court discussed conclusory statements in *Gates*. Conclusory statements can be used in search warrants, as long as, the conclusory statements are not to such an extent that there is no basis for probable cause. "A sworn statement of an affiant that "he has cause to suspect and does believe that" liquor illegally brought into the United States is located on certain premises will not do. *Nathanson v. United States,* 290 U.S. 41, 54 S.Ct. 11, 78 L.Ed. 159 (1933). An affidavit must provide the magistrate with a substantial basis for determining the existence of probable cause, and the wholly conclusory statement at issue in *Nathanson* failed to meet this requirement." *Gates* at 239. When discussing conclusory statements in *Gates*, the Supreme Court was dealing with statements that were wholly conclusory, without any supporting facts, leaving the magistrate with, "virtually no basis at all for making a judgment regarding probable cause." *Id* at 239. That is not the case with search warrant for the defendant's home. It contained sufficient detail, supported by facts, that connected the home to the crime.

D. The Good Faith Exception

Even if this Court held that the warrant was not based upon probable cause, the motion to suppress evidence should still be denied because the law enforcement officers executing the warrant acted in good faith and reasonably relied upon the warrant issued by the St. Louis County Judge. There is a "good faith" exception to the exclusionary rule where evidence was obtained based upon a warrant that was signed by a judge but that is later found to lack probable cause. *United States v. Leon*, 468 U.S. 897 (1984). Evidence should not be suppressed "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." *Id.* at 921. "The marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion." *Id.* at 921. SI Becker monitored the information he got from the law enforcement version of Freenet based on his training and experience. The information SI Becker provided to Det. Slaughter he knew and believed to the true and correct. Det. Slaughter then relied on that information in good faith and properly obtained a search warrant from a St. Louis County Judge. The search warrant was executed properly on the defendant's home and evidence was seized accordingly. Therefore, even if the Court finds that the search warrant lacks probable cause, the motion to suppress should still be denied based on the good faith exception.

IV. CONCLUSION

The defendant's motion to suppress should be denied. There is no misleading or false information contained in the search warrant affidavit. The omissions as to specific data regarding the investigation into the defendant on Freenet only bolster the probable cause for the search warrant when supplemented. Further, these details were not left out of the search warrant affidavit to mislead the judge. The St. Louis County Judge who read the search warrant was neutral and capable of reviewing the affidavit, making a decision, and signing the search warrant. The law enforcement officers who performed the investigation in this case and who swore to the affidavit did so in good faith.

Respectfully submitted,

RICHARD G. CALLAHAN
United States Attorney
s/ Colleen Lang
COLLEEN LANG, 56872MO
Assistant United States Attorney
111 South 10th Street, Room 20.333
St. Louis, MO 63102
(314) 539-2200

CERTIFICATE OF SERVICE

I hereby certify that on November 21, 2016, the foregoing was filed electronically with the Clerk of the Court. The foregoing was emailed to counsel of record for the defendant.

s/ Colleen Lang
COLLEEN LANG, 56872MO
Assistant United States Attorney